CSCI 404/604 Ethical Hacking

North Dakota State University

Spring 2021

Riley Abrahamson

Joshua Gisi

Alison Gonser

Jeremy Rylicki

Zachary Miller

Geri Shaeffer

# Abstract

In the modern, connected enterprise, security awareness generally takes the form of mandatory training assigned to each user in the organization. Information Technology Security and/or designated training personnel typically assign users annual training centered around commonly recognized security threats[[1]](#footnote-0).

Although many engaging and effective security awareness programs exist, it is still a challenge to persuade an individual to fully engage with their security awareness courses, retain the knowledge effectively, and implement the prescribed secure behaviors that assist the organization in avoiding security threats. In many cases, users complete the minimum required training and often feel that the programs are a hindrance to actual work being accomplished[[2]](#footnote-1). In order to facilitate increased employee engagement, the concept of mandatory annual security training should be enhanced via the incorporation of game-like qualities otherwise termed as “Gamification.”

Gamification, in this domain, takes the form of presenting security awareness training materials and allows users to play games based upon various cybersecurity scenarios. This not only makes security awareness entertaining and engaging, but it prepares employees for a real security threat in the future[[3]](#footnote-2). Gamification gives individuals an additional reason to complete tasks that they otherwise feel difficult, uninteresting, or unimportant to the individual[[4]](#footnote-3)3. Turning a mandatory task into an enjoyable game transforms completing a task into an enjoyable activity[[5]](#footnote-4)3.

# Introduction

## Social Engineering

Social Engineering is the term used for a wide range of malicious activities accomplished through human interactions[[6]](#footnote-5). Social Engineering describes attempts at utilizing psychological manipulations to persuade users into making security gaffes and, therefore, divulge sensitive information. These attacks tend to be quite effective and are quite common, primarily because of human nature and the desire to be helpful[[7]](#footnote-6).

Social Engineering attacks tend to be multifaceted in approach. A malicious agent will first investigate their target to gather the required background information, such as potential openings and/or vulnerabilities in the observed security procedures, necessary for an attack. The agent then attempts to gain the target’s confidence and provide enticements for revealing sensitive information and/or potentially granting access to critical resources. These attacks are often devastating because they are difficult to guard against, as it is the users themselves willingly granting the malicious actor unauthorized resource access. Errors made by the target are much less foreseeable, rendering them harder to detect and impede than a malware-based intrusion.

There are several common types of Social Engineering tactics[[8]](#footnote-7):

* *Baiting* attacks utilize false guarantees to lure the target by enticing them through curiosity or a reward. The agent will provide seemingly authentic software, which is actually malware, with hopes for execution on the target systems.
* *Scareware* involves deception via false alarms and empty threats. The targets are deceived into believing their system is infected with malware. At that point, the target is instructed to install additional software that is malware itself.
* *Pretexting*involves deception via requests originating from malicious actors who create elaborate backstories in order to masquerade as entities who are normally considered privileged to view the resources sought after by the attack.
* *Phishing* generally takes the form of email and text message campaigns intending to generate a sense of urgency, curiosity, or fear in the target. Once the target engages with the message, the malicious agent will request immediate action, often via the clicking of a spoofed URL leading to a malicious website, which aims to steal credentials.
* *Spear phishing* involves a malicious agent and a well-researched target. The malicious agent imitates a user or entity considered trustworthy to the well-researched target, and then prompts the recipients to divulge sensitive information via the usage of malicious websites and/or other means.

*Fake News* is a social engineering strategy that uses malicious news content masquerading as content originating from authoritative sources. Fake News purveyors seek to deliberately misinform users and/or cause viral spread of content that is designed to elicit outrage and/or change opinions. From a cybersecurity perspective, fake news can cause its inadvertent consumers to form opinions that may be detrimental to an enterprise. A coordinated fake news attack on an organization may result in serious financial implications for the target firm7.

Impacts of Social Engineering 8

* **Financial Losses**

Through a multitude of factors, the actions of malicious actors running a successful social engineering strategy may cause significant financial losses to an enterprise. These factors range from the direct theft of funds from bank accounts, to losses stemming from the inability to conduct business, and even damage to the reputation of a firm. There is also significant cost associated with upgrading operational security and repairing damages.

* **Loss of Productivity**

A successful attack may result in significant resources being reallocated to correct and repair the damages rendered upon the firm. Remedial cybersecurity education programs will require employee time, rather than allowing focus on normal job duties.

* **Operational Disruption**

These incidents often derail the enterprise from its core competencies and, instead, divert resources to address the matter. This diversion results in disruptions to many, if not all, aspects of the enterprise.

* **Reputational Damage**

Cybersecurity attacks are extremely dangerous, as they put both organizations and customer data at risk. If an organization is not seen as adequately protected, then the internal/external stakeholders may have a diminished opinion of the overall capability of the enterprise.

## Project Overview

The purpose of this project is to increase awareness of the concept of Social Engineering and its impacts upon the broader topic of Cyber Security. We will attempt to gain insight into individuals’ current knowledge of social engineering tactics and their experiences with these types of situations. To attempt to measure this, we will accumulate data about how individuals identify and react to social engineering situations and tactics. The goal is to answer the following questions:

* What are some of the most effective social engineering tactics?
* Is there a certain group of people more susceptible to social engineering attacks?
* How do people respond to social engineering attempts?
* Do people identify social engineering?

The main methodology of this project is to establish a baseline of an individual's knowledge of social engineering practices and record their responses to the simulated situations. We will collect the majority of the data through a survey and scenarios process related to social engineering. We will use a pre-survey to gather demographics, such as age, current knowledge of social engineering, prior cyber security training, and other related topics. The survey will be followed by social engineering scenarios in which the user will be asked to read the scenario and reply with their reaction to the situation.

After the scenarios, we will provide a segment that seeks to educate the user on social engineering and various tactics they may encounter. We intend to also provide an educational aspect to our research with the purpose of educating users on social engineering tactics and help them be better prepared to defend against these types of attacks. We will include a post-survey to measure the education they received and their response to a simulated sophisticated social engineering attack.

To test the user’s social engineering identification abilities, an interactive hacking-oriented game will be provided. This game will allow users to test their skills in balancing workplace technology safety with accomplishing normal daily tasks. This game will incorporate gamified representations of social engineering techniques which players can complete in order to earn points. This will keep users more engaged than conventional slideshow-based learning modules and encourage players to practice multiple times out of sheer enjoyment. The game will be built in *GameMaker Studio 2*.

## Project Objectives

The objectives of this project are the following:

* Increase awareness of social engineering and how it relates to cyber security.
* Determine what types of social engineering tactics are effective.
* Collect data on how people identify and react to social engineering scenarios.

A pre-survey will be used to establish a baseline regarding social engineering knowledge and obtain key demographics. A post-survey will be used to gain insight into the user experience and assess knowledge and key takeaways. The score of the game will also be provided.

Once the survey results have been collected as fully as possible, the data will be analyzed in order to determine if there is a trend towards certain demographic groups of users that are more susceptible to social engineering attempts. This will attempt to determine whether or not different demographics could be more vulnerable to attack, particularly older age groups. The rationale behind this is that some age groups were born into a technology age versus others who were not. The data will be analyzed to determine if this theory is correct. If so, then perhaps future endeavors at gamification of cyber security educational materials can adjust the material based upon perceived risk factors of the demographic group that the user is in.

## Proposed System

* 1. System needs and requirements

The scenario survey needed to include scenarios that were plausible social engineering attempts. Each scenario required that the participants would be able to make a decision based solely upon their knowledge and instincts rather than being led to a specific response by leading words in the scenarios. The scenarios also needed to provide enough description and information for participants to understand and respond to the scenarios accurately. The scenario survey also required a way to determine if participants could identify social engineering attempts with their current knowledge and also after being provided with knowledge on social engineering.

The simulation was devised to provide a way for research participants to both 1. Showcase any skills they already possessed in good security practices or to 2. Provide an experiential way to learn lessons related to social engineering tactics. In both of these cases, the simulation had several design goals in mind. Most prominently, it needed to be easy to interact with and accessible on a wide range of devices. Additionally, the simulation needed to adequately demonstrate skills in the workplace at preventing or avoiding social engineering attempts. Lastly, the simulation needed to feel properly gamified. Workplace technology safety training is often dry and monotonous; a more interactive design was brainstormed to keep research participants engaged throughout the entire study.

* 1. System design

The scenario survey was designed to include two sets of five social engineering scenarios. Each set included scenarios of potential real-world social engineering attempts covering the following social engineering tactics: shoulder surfing, phishing, tailgating, scareware, and baiting. A question was included with each scenario asking if the participant would proceed in a designated manner. An answer of yes or no was provided for each scenario question. An answer of yes to any of the scenarios indicated that the participant would or potentially would be susceptible to the type of social engineering presented. The following lists the scenarios and questions in the order in which they were presented to participants.

* **Scenario 1 - Shoulder Surfing**

You are attending a business convention and meet someone who tells you that they work for the same company at one of the branch locations. You spend time talking with this individual over the course of the convention and you ask if this individual’s branch has upgraded their online system yet. The individual replies that they haven’t yet, but they can’t wait to use it. You have your laptop on so you offer to show them some of the new features. They get up and stand behind you so that they can see your screen. You open up your company’s system and the login screen appears.

Would you continue to type in your username and password?

* **Scenario 2 - Phishing**

You have a movie streaming account and regularly use this service to watch movies and tv shows. You receive an email with the subject line “Update account information” from support@emailer.com. The email states the following: *Hello valued customer,* *Your payment method for your account needs to be updated in order to continue using our services. We currently are unable to authorize your last payment due to an issue with your credit card on file. Please click the link below to verify that your payment information is correct or to update with a new payment method. If you have any questions or concerns please contact customer service.* You can’t remember what card you used to pay for this streaming service. The email contains the streaming service’s logo and all spelling and grammar is correct.

Would you click on the link to update/verify your payment information?

* **Scenario 3 - Tailgating**

You work for a company with a large office building where all visitors must sign the visitor log and be escorted by an employee while in the building. All entrances to the building require an employee badge to enter. One day as you are coming back from lunch you walk toward the employee entrance in the back of the building and scan your badge to get in. As you are opening the door you notice an individual walking up to the door holding several boxes and bags that are from a local office supply store. This individual is struggling with the number of items and is also trying to reach into their pocket to retrieve something.

Would you hold the door open for this individual?

* **Scenario 4 - Scareware**

You have been working on your computer for several hours with various applications and web browsers open. As you switch between various windows a large popup appears on your screen with a smaller popup in front of it. The large popup has the title “WINDOWS VIRUS WARNING!” and underneath a list of alerts that you see contain words like trojan and spyware. It also says that it has detected 23 viruses that pose a threat to your system. The smaller popup on top of this says “Your computer has been locked. Windows has detected a virus attack on your computer. Contact Windows Security Help Line.” The large and small popup both contain a 1-800 number for the help line. You can close out of the smaller popup but you can’t click or interact with anything else on your computer screen.

Would you call the 1-800 number listed?

* **Scenario 5 - Baiting**

You are doing research at a local university and one day as you are walking toward the research building you notice a USB drive on the sidewalk outside the building. The USB is the same type that you use in the lab for transferring data. You pick it up and notice a label on it that reads “2018-2021 data results”. There is nothing to indicate the owner of the USB drive. You decide to not leave the USB drive outside so you bring it into the research building with you.

Would you plug this USB drive into a computer to view it’s content?

* **Scenario 6 - Shoulder Surfing**

You work remotely for a company and are responsible for managing the company's financial transactions. You work mainly from home, but you find it easier to get more work done by going elsewhere. You usually go to a nearby coffee shop with your laptop. Today the shop is busier than usual with almost every table full so you find a seat at a table in the center of the shop. You need to access the company’s bank statements online through the bank’s website where your company has their account. You navigate to the bank’s website and the login screen appears requesting your username and password.

Would you continue with entering your username and password to login?

* **Scenario 7 - Phishing**

You don’t have a laptop or desktop computer so you access websites and applications on your cell phone. You have a social media account that you access frequently. One day you receive an email with the following message regarding your social media account: *Hello,* *A new device has been used to access your account at 1:13pm today.* *Operating System: Mac OS X 10.5* *Browser: Safari* *Location: Amsterdam, NH, NL* *If you did this, you may ignore this message.* *If you did not access your account with this device please secure your account by following the link listed below.* *Sincerely,* *Customer Security Team;* You have only used your phone to access your account and you don’t have a Mac OS device nor have you been in the location listed.

Would you click on the link to access your account in order to secure it?

* **Scenario 8 - Tailgating**

There are many employees at your office and you only know a handful of them by name and which department they work in. You always use the employee entrance that requires a keycard to get in. One day while walking to the door an individual rushes up behind you as you scan your keycard. You recognize their face as you have seen them sitting outside at the employee picnic table on several occasions eating lunch. You have never spoken to this individual but only observed them in passing. They look stressed and in a hurry. They say, “Hey, can you please hold the door? My kid had an accident this morning and it put me out of sorts and I forgot my keycard. I’m late for a meeting that I can’t miss.”

Would you let this individual enter the building with you?

* **Scenario 9 - Scareware**

You have an issue with your printer and are searching the internet on your laptop for a solution to get it working. You really need to print off some documents so you have been clicking on any site that may give you a solution. You find a promising yet unfamiliar site and you click on the link. Once you click on the link and get redirected to the site a pop up banner appears at the top of your browser with the following message: “A harmful spyware program has been detected on your computer. Click here to remove harmful programs using the free trial of CleanSpyware removal tool.” Currently your computer doesn’t have any antivirus or security software installed to take care of risks.

Would you click to remove the detected spyware using the CleanSpyware removal tool offered?

* **Scenario 10 - Baiting**

You are a huge fan of a popular tv series that you were able to view on a streaming service. Unfortunately, the series was removed from the streaming service before you could finish the last few episodes. The last episode that you were able to watch left off on a huge cliffhanger and you desperately want to find out what happens next. There currently isn’t any streaming service that you know of that has this series available. You have been browsing the internet on your cell phone to find where you can watch the last few remaining episodes. You find a site that says that you can watch all the full episodes of the series that you were looking for. It has a download link for each of the seasons. You see that it has a link for the last season that you want to watch.

Would you click on the link to watch the episodes that you missed?

In the simulation, the user takes the role of an office worker bombarded by tasks related to business work and social engineering. The user must interact with the tasks to score points thus showing their understanding of social engineering tactics and ability to adapt to unforeseen risks. The simulation is designed as a project in *GameMaker Studio 2*, as this tool is easy to teach, produces playable content very quickly, and scales well across multiple device environments. The simulation for this research study was specifically produced as a web project, meaning any browser for a desktop computer could access the simulation.

* 1. System operations

The scenario survey begins with basic demographic questions. After the demographic questions, five scenarios are presented to participants with a question if they would proceed in a certain manner. After the first five scenarios, the participants read through an education section that includes the definition of social engineering and the types of social engineering presented in the scenarios. Information on ways to prevent and avoid these types of attacks is also presented. After the education section, the participants are presented with an additional five scenarios that differ from the first five but cover the same type of social engineering attempt.

The simulation operates over three screens. The first is a short screen detailing the project’s title, creators, and a basic set of instructions. Once the user is ready, they are moved to the main interactive screen. Here the user takes the role of an office worker for three minutes. As office workers, they will interact with a variety of tasks in their office space by clicking with their mouse cursor. The tasks reflect social engineering techniques, such as phishing emails showing up on the user’s computer alongside genuine business emails. Successfully interacting with office tasks and catching attempts in the act awards points, whereas falling victim to the subterfuge subtracts points. After the three minutes are up, the user is moved to a new screen where they are provided their score.

## Project Evaluation

* 1. Experimental methodology

Participants were recruited from the North Dakota State University research participant list. An email was sent to the individuals included in this list with an invitation to participate in this research. The email included the intent of the research with two links, one for the survey with the scenarios and one for the survey with the simulation. Participants were allowed to complete either or both of the surveys. The surveys were made active through Qualtrics, an online survey tool, and remained active for six days to collect participant responses.

* 1. Data and analysis

Responses were collected from 106 participants for the survey of social engineering scenarios. The majority of participants were in the 18-24 age range with 82 participants. Nineteen participants were in the 25-34 age range and the remaining four were between 35 and 64. There were a total of 64 female participants, 36 male participants, 1 indicating other gender, and 5 who preferred not to say.

Table 1. Total Participants By Gender and Age Group

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Gender\Age | 18-24 | 25-34 | 35-44 | 45-54 | 55-64 |
| Male | 26 | 8 | 1 | 1 | 0 |
| Female | 51 | 11 | 1 | 0 | 1 |
| Other | 1 | 0 | 0 | 0 | 0 |
| Prefer not to say | 4 | 0 | 1 | 0 | 0 |

After the education section of the survey, there was a decrease in the percentage of overall participants who answered yes for all the scenarios except for the scenarios about phishing. For the phishing scenario, there was an increase in the percentage of “yes” responses after the education section. The tailgating scenario had the most yes responses before and after the education out of all the scenario types.

Table 2. Percentage Yes Responses Pre-Education Versus Post-Education

|  |  |  |
| --- | --- | --- |
| Scenario Type | Pre-Education | Post-Education |
| Shoulder Surfing  Scenario 1 & 6 | 25.5% | 16.0% |
| Phishing  Scenario 2 & 7 | 17.9% | 24.5% |
| Tailgating  Scenario 3 & 8 | 68.9% | 33.0% |
| Scareware  Scenario 4 & 9 | 13.21% | 3.8% |
| Baiting  Scenario 5 & 10 | 19.8% | 11.3% |

The majority of participants were in the age range of 18-24 with 82 participants. There were 19 participants in the age range 25-34, 3 in the age range 35-44, and 1 in both the 45-54 and 55-64 age range.

In the 18-24 and 25-34 age range Scenario 3 & 8 - Tailgating had the highest percentage of yes responses out of all the pre-education and post-education scenarios. For both these age ranges there was a decrease in the percentage of yes responses for the post-education scenarios except for Scenario 7 - Phishing. This scenario had an increase in percentages of yes responses for the post-education scenarios in the 18-24 age range and the same percentage in the 25-34 age range.

Table 3. Percentage Yes Responses By Age Group

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Age | 18-24 | 25-34 | 35-44 | 45-54 | 55-64 |
| Total | 82 | 19 | 3 | 1 | 1 |
| Scenario 1 | 25.6% | 21.1% | 66.7% | 0.0% | 0.0% |
| Scenario 2 | 22.0% | 5.3% | 0.0% | 0.0% | 0.0% |
| Scenario 3 | 74.4% | 57.9% | 0.0% | 0.0% | 100.0% |
| Scenario 4 | 14.6% | 10.5% | 0.0% | 0.0% | 0.0% |
| Scenario 5 | 23.2% | 10.5% | 0.0% | 0.0% | 0.0% |
| Scenario 6 | 18.3% | 5.3% | 33.3% | 0.0% | 0.0% |
| Scenario 7 | 29.3% | 5.3% | 33.3% | 0.0% | 0.0% |
| Scenario 8 | 34.1% | 31.6% | 33.3% | 0.0% | 0.0% |
| Scenario 9 | 4.9% | 0.0% | 0.0% | 0.0% | 0.0% |
| Scenario 10 | 12.2% | 5.3% | 33.3% | 0.0% | 0.0% |

The majority of participants were female with 64 participants. There were 36 male participants, 1 indicating another gender, and 5 who preferred not to say.

For males and females, Scenario 3 & 8 - Tailgating had the highest percentage of yes responses out of all the pre-education and post-education scenarios. For both genders, there was a decrease in the percentage of yes responses for the post-education scenarios except for Scenario 7 - Phishing. This scenario had an increase in percentages of yes responses for the post-education scenarios for both males and females.

Table 4. Percentage Yes Responses By Gender Group

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gender | Male | Female | Other | Prefer not to say |
| Total | 36 | 64 | 1 | 5 |
| Scenario 1 | 25.0% | 25.0% | 100.0% | 20.0% |
| Scenario 2 | 11.1% | 21.9% | 0.0% | 20.0% |
| Scenario 3 | 63.9% | 70.0% | 100.0% | 80.0% |
| Scenario 4 | 5.6% | 18.8% | 0.0% | 0.0% |
| Scenario 5 | 16.7% | 21.9% | 0.0% | 20.0% |
| Scenario 6 | 16.7% | 15.6% | 0.0% | 20.0% |
| Scenario 7 | 25.0% | 25.0% | 0.0% | 20.0% |
| Scenario 8 | 27.8% | 31.3% | 100.0% | 80.0% |
| Scenario 9 | 0.0% | 6.3% | 0.0% | 0.0% |
| Scenario 10 | 8.3% | 12.5% | 0.0% | 20.0% |

The majority of participants indicated that they did not have any prior security training with a total of 74 participants. Thirty-one indicated that they had security training and one participant preferred not to say if they had training or not.

The percentage of those who answered yes to the scenario questions and had security training was lower in seven scenarios when compared to those who had no security training. Scenario 3 and Scenario 8 - Tailgating had the highest percentage of yes responses for both those who indicated having security training and those who indicated not having security training. For those who had security training there was a decrease in the percentage of yes responses for the post-education scenarios except Scenario 1 - Shoulder Surfing and Scenario 7 - Phishing for which both increased. Scenario 4 and 9 - Scareware remained the same at 0%. For those who did not have security training, there was a decrease in the percentage of yes responses for the post-education scenarios except Scenario 7 - Phishing which increased.

Table 5. Percentage Yes Responses By Having Security Training

|  |  |  |  |
| --- | --- | --- | --- |
| Has Security Training | Yes | No | Prefer not to say |
| Total | 31 | 74 | 1 |
| Scenario 1 | 19.4% | 28.4% | 0.0% |
| Scenario 2 | 9.7% | 20.3% | 100.0% |
| Scenario 3 | 48.4% | 77.0% | 100.0% |
| Scenario 4 | 0.0% | 18.9% | 0.0% |
| Scenario 5 | 19.4% | 18.9% | 100.0% |
| Scenario 6 | 22.6% | 13.5% | 0.0% |
| Scenario 7 | 29.0% | 23.0% | 0.0% |
| Scenario 8 | 32.3% | 32.4% | 100.0% |
| Scenario 9 | 0.0% | 5.4% | 0.0% |
| Scenario 10 | 3.2% | 13.5% | 100.0% |

The majority of participants indicated that their highest level of education was some college with 59 participants. Participants with a bachelor’s degree included 25 participants, post-graduate degree 12, associate’s degree 8, and high school 2.

For those with their highest level of education being some college, associate’s degree, bachelor’s degree, and post-graduate degree Scenario 3 and Scenario 8 - Tailgating had the highest percentage of yes responses. For those who had some college or bachelor’s degree, there was a decrease in the percentage of yes responses for the post-education scenarios except Scenario 7 - Phishing for which both increased. For those with an associate’s degree Scenario 1 and Scenario 6- Shoulder Surfing and Scenario 2 and Scenario 7 - Phishing remained the same. For those with a postgraduate degree Scenario 2 and Scenario 7 - Phishing remained the same, Scenario 3 and Scenario 8 - Tailgating remained the same, Scenario 4 and Scenario 9 - Scareware remained the same, and Scenario 5 and Scenario 10 - Baiting remained the same.

Table 6. Percentage Yes Responses By Highest Level of Education

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Highest level of Education | High School | Some College | Associate’s Degree | Bachelor’s Degree | Postgraduate Degree |
| Total | 2 | 59 | 8 | 25 | 12 |
| Scenario 1 | 50.0% | 25.4% | 25.0% | 24.0% | 25.0% |
| Scenario 2 | 50.0% | 22.0% | 37.5% | 8.0% | 0.0% |
| Scenario 3 | 100.0% | 72.9% | 100.0% | 60.0% | 41.7% |
| Scenario 4 | 0.0% | 16.9% | 37.5% | 4.0% | 0.0% |
| Scenario 5 | 50.0% | 22.0% | 25.0% | 16.0% | 8.3% |
| Scenario 6 | 50.0% | 16.9% | 25.0% | 8.0% | 16.7% |
| Scenario 7 | 0.0% | 28.8% | 37.5% | 20.0% | 8.3% |
| Scenario 8 | 0.0% | 33.9% | 62.5% | 20.0% | 41.7% |
| Scenario 9 | 0.0% | 3.4% | 25.0% | 0.0% | 0.0% |
| Scenario 10 | 50.0% | 13.6% | 12.5% | 4.0% | 8.3% |

The survey containing the simulation returned 112 respondents. However, of those 112 participants who took the survey, only 88 of them provided a score for their attempt at playing the simulation. Additionally, four of the responses were not valid score numbers and instead were descriptive text responses. Therefore, 84 participant scores were counted for data analysis.

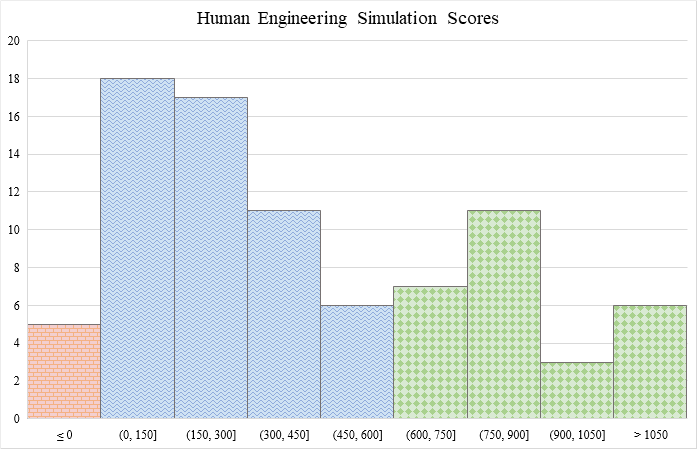
The reported scores can be divided into 3 primary categories, shown in the chart as three separate color-pattern groupings.

The first category consists of all scores below or equal to 0. These five respondents were unable to finish the simulation correctly and did not earn any points. This showcases either a lack of domain knowledge and familiarity with social engineering techniques or a misunderstanding of how to interact with the simulation. These account for a little over 5% of the responses, which indicate that a large majority of participants understood how to play and interact in-browser. Therefore we could assume that these low scores are connected to the lack of domain knowledge.

The next category consists of scores greater than 0, but less than 600. Six-hundred was the calculated baseline for players who used the simulation. It represents an expected score for a player who is mildly familiar with social engineering techniques and flexible enough to adapt to the simulation environment within three minutes. Participants in the 0-600 range showed some understanding of the material but maybe were unable to connect it to the simulation or learn the simulation’s interactions and tasks quickly enough. This was the largest chunk of returned scores at nearly 60% of all participants.

Lastly, the final category consists of scores that met and exceeded the baseline score of 600. These were considered exemplary scores and demonstrated a well-rounded grasp of the content material and gameplay of the simulation. This accounted for about 30% of respondents. The top score reported was 1350, or approximately 85 completed tasks.

Chart 1. Human Engineering Simulation Scores



The breakdown for participants shows that a majority of responses came from individuals in the 18-24 age range.The survey and simulation were delivered via the university research email, which means the primary audience receiving the links would be young adults in college. The survey also had an even breakdown of male and female participants, with 49 respondents responding male and 56 responding female.

Table 7. Total Participants By Gender and Age Group

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Gender | 18-24 | 25-34 | 35-44 | 45+ | Prefer not to say |
| Male | 36 | 10 | 3 | 0 | 0 |
| Female | 44 | 12 | 0 | 0 | 0 |
| Non-binary / third gender | 2 | 0 | 0 | 0 | 0 |
| Prefer not to say | 4 | 0 | 0 | 0 | 1 |

Looking at the first major demographic compared to score, we see that the youngest age grouping covered all ranges for scores. While the scores clustered around the second category specified in Chart 1, there were notable numbers around the cut-off of 600+. The youngest age group also notably had the only responses that exceeded 100 points and crossed into the largest bins of scores.

Table 8. Score Category By Age

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Age | 18-24 | 25-34 | 35-44 | 45+ | Prefer not to say |
| Total | 86 | 22 | 3 | 0 | 1 |
| ≤ 0 | 4 | 1 | 1 | 0 | 0 |
| (0-150] | 13 | 4 | 0 | 0 | 0 |
| (150-300] | 12 | 4 | 0 | 0 | 0 |
| (300-450] | 11 | 1 | 0 | 0 | 0 |
| (450-600] | 3 | 3 | 0 | 0 | 0 |
| (600-750] | 7 | 1 | 0 | 0 | 0 |
| (750-900] | 9 | 0 | 1 | 0 | 0 |
| (900-1050] | 3 | 0 | 0 | 0 | 0 |
| > 1050 | 6 | 0 | 0 | 0 | 0 |
| Text Response | 3 | 0 | 1 | 0 | 0 |
| No Response | 15 | 8 | 0 | 0 | 1 |

As for the gender breakdown, there are a few observable trends. Male participants had larger spikes at individual tiers, creating a more erratic pattern. Meanwhile, female participants had a more even slope of scores overall. An additional note is that one of the highest achieved scores was reported by an individual who chose not to list their gender, but did list other demographic information. This was uncommon as those who chose “Prefer not to say” typically chose that option for nearly all of the fields.

Table 9. Score Category By Gender

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Gender | Male | Female | Non-binary / third gender | Prefer not to say |
| Total | 49 | 56 | 2 | 5 |
| ≤ 0 | 2 | 3 | 0 | 0 |
| (0-150] | 10 | 6 | 0 | 2 |
| (150-300] | 8 | 9 | 0 | 0 |
| (300-450] | 3 | 8 | 0 | 0 |
| (450-600] | 2 | 4 | 0 | 0 |
| (600-750] | 3 | 4 | 0 | 0 |
| (750-900] | 6 | 4 | 1 | 0 |
| (900-1050] | 1 | 2 | 0 | 0 |
| > 1050 | 3 | 2 | 0 | 1 |
| Text Response | 2 | 2 | 0 | 0 |
| No Response | 9 | 12 | 1 | 2 |

One of the demographics the study was most concerned with was whether study participants had any previous education in technology security and social engineering. The hypothesis was that those who did would perform better in the simulation compared to those that didn’t; they would have greater familiarity with social engineering techniques and respond quicker in the three minute span.

For the responses, there was fewer than two-times the number of participants who had never received security training. Whether due to shear numbers or other factors, this demographic actually captured five of the six > 1050 scores as opposed to those that had prior security training. Otherwise, the scores were fairly similar between the two groups, especially considering the numbers in each demographic.

Table 10. Score Category By Having Security Training

|  |  |  |  |
| --- | --- | --- | --- |
| Has Security Training | Yes | No | Prefer not to say |
| Total | 39 | 72 | 1 |
| ≤ 0 | 1 | 4 | 0 |
| (0-150] | 6 | 12 | 0 |
| (150-300] | 3 | 14 | 0 |
| (300-450] | 7 | 4 | 0 |
| (450-600] | 2 | 4 | 0 |
| (600-750] | 2 | 5 | 0 |
| (750-900] | 5 | 6 | 0 |
| (900-1050] | 1 | 2 | 0 |
| > 1050 | 1 | 5 | 0 |
| Text Response | 0 | 3 | 0 |
| No Response | 10 | 13 | 1 |

Finally, the study also attempted to find any correlations between participant education levels and simulation performance. The "some college” demographic had the largest number of >1050 scores, but it was also larger than every other education demographic combined. Another outlier is that 23% of those with a postgraduate degree achieved a score of zero or less. This could be an indication that higher education isolated from specified security training isn’t enough protection against hacking attempts.

Table 11. Score Category By Highest Level of Education

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Highest level of Education | High School Graduate | Some College, No Degree | Associate’s Degree | Bachelor’s Degree | Postgraduate Degree | Prefer Not to Say |
| Total | 5 | 56 | 8 | 28 | 13 | 2 |
| ≤ 0 | 0 | 4 | 0 | 1 | 3 | 1 |
| (0-150] | 1 | 6 | 1 | 6 | 0 | 0 |
| (150-300] | 2 | 10 | 0 | 4 | 1 | 0 |
| (300-450] | 0 | 7 | 1 | 3 | 0 | 0 |
| (450-600] | 0 | 2 | 0 | 2 | 2 | 0 |
| (600-750] | 0 | 3 | 2 | 2 | 0 | 0 |
| (750-900] | 0 | 5 | 2 | 3 | 1 | 0 |
| (900-1050] | 0 | 2 | 1 | 0 | 0 | 0 |
| > 1050 | 0 | 4 | 0 | 2 | 0 | 0 |
| Text Response | 0 | 2 | 0 | 1 | 1 | 0 |
| No Response | 2 | 11 | 1 | 4 | 5 | 1 |

* 1. System evaluation

From the scenario survey it was shown that there was an overall decrease in “Yes” responses after participants were educated on social engineering. The scenario involving phishing did not have a decrease in “Yes” responses after the education section but rather an increase. When evaluating specific demographic categories where there were more than five participants the scenario involving phishing had an increase or no change in percentages of “Yes” responses after the education section. The scenarios related to tailgating had the highest percentage of “Yes” responses overall and for each evaluated demographic category where there were more than five participants.

The simulation side of the research project drew some interesting connections between the participants and their scores. Namely, fewer participants scored the baseline of 600 than expected. Assumptions had been that this would be easy to reach and would form the peak of a bell curve for the scores. The peak of the curve formed around the (0-150] and (150-300] score silos. Additionally, there were not any clear, direct correlations between education/training and performance in the simulation. This could be the result of many details of the research project, but a larger (and more diverse) sample size would have assisted with discerning whether the discrepancies lied with the participants or the simulation.

## Conclusion

* 1. Importance of the system

The scenario survey was important in gaining insight into effective social engineering tactics, how people respond to social engineering attempts, and if people identify social engineering.

The scenario survey indicates that education can be an important factor in helping individuals to identify and prevent social engineering attempts. The scenario survey can also be used to help understand what types of social engineering tactics may be the most effective and the least likely to be detected or avoided.

The simulation helped provide a way for participants to display and test their skills in an experiential environment. Additionally, given nearly two-thirds of participants had not had prior security training, the simulation served an important first-step in the path of IT security and safety for these individuals. The simulation scoreline indicates that extra education would be valuable in the key largest demographics from this study, as well as additional education into crafting more immersive simulations for training purposes.

* 1. What has been presented in the paper

This paper has presented social engineering and its consequences, the need to increase awareness on social engineering, and the research completed to gain insight into social engineering. The methods, details, and processes for completing this research was also covered along with the collected data and its analysis.

* 1. System evaluation conclusions

From the scenario survey it was not able to be determined if a certain demographic is more susceptible to social engineering attempts than others. This was due to the participants recruited being mainly of the same demographic. With more participants being from different demographics especially age, there could potentially be insight gained into the correlation between demographics and susceptibility.

Education was shown to be a potential factor in how participants responded to social engineering attempts. It was concluded as a result of the post-education scenarios having a lower percentage of yes responses that education is beneficial to identifying social engineering attempts.

The increase in percentage of yes responses for the post-education phishing scenario could potentially indicate that it isn’t as easily identifiable as other social engineering attempts. This would make phishing an effective social engineering tactic. Tailgating also appears to be an effective social engineering tactic. Only assumptions can be made as to why these two types of tactics are effective or potentially effictive. No user comments were collected to determine reasons for participants' responses.

* 1. System immediate next steps

There are no immediate next steps that will be taken for the scenario survey nor for the simulation.

* 1. Future work

No future work is presently planned for this research, but there is potential for it to be extended and built upon. In order to determine if a certain demographic is more susceptible to social engineering attempts the research could recruit more participants from a wider age range. If determining the effectiveness of different types of social engineering attempts is desired this research could be extended to include tactics not already included. Comments could also be gathered from participants to determine why they made certain decisions and to also give insight into why certain tactics are more effective than others.

## Acknowledgements

* Research Adviser

Jeremy Straub, Ph. D.

Assistant Professor of Computer Science

Associate Director of the Institute for Cyber Security Education and Research

## References

[1] Security Magazine. (2020, October 6). 65% of leaders say that security awareness training is not a top priority. Security Magazine RSS. https://www.securitymagazine.com/articles/93528-of-leaders-say-that-security-awareness-training-is-not-a-top-priority.

[2] Society for Human Resource Management (SHRM). (2016). EMPLOYEE JOB SATISFACTION AND ENGAGEMENT Revitalizing a Changing Workforce. https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/2016-Employee-Job-Satisfaction-and-Engagement-Report.pdf. shrmstore.shrm.org.

[3] Rieff, I. (2018). Systematically Applying Gamification to Cyber Security Awareness (thesis).

[4] Social Engineering Defined. Security Through Education. (2020, December 19). https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/.

[5] F. Mouton, M. M. Malan, L. Leenen and H. S. Venter, "Social engineering attack framework," 2014 Information Security for South Africa, 2014, pp. 1-9, doi: 10.1109/ISSA.2014.6950510.

[6] Ivaturi, K., & Janczewski, L. (2011, June). A Taxonomy for Social Engineering attacks. http://aisel.aisnet.org/confirm2011.

[7] A. Bedi, N. Pandey and S. K. Khatri, "A Framework to Identify and secure the Issues of Fake News and Rumours in Social Networking," 2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC), 2019, pp. 70-73, doi: 10.1109/PEEIC47157.2019.8976800.

[8] Forbes. (2014). IBM\_Reputational\_IT\_Risk\_REPORT. Forbes Insights. https://images.forbes.com/forbesinsights/StudyPDFs/IBM\_Reputational\_IT\_Risk\_REPORT.pdf.

1. Security Magazine [↑](#footnote-ref-0)
2. SHRM, [↑](#footnote-ref-1)
3. Rieff [↑](#footnote-ref-2)
4. Social Engineering [↑](#footnote-ref-3)
5. F. Mouton [↑](#footnote-ref-4)
6. Ivaturi, K [↑](#footnote-ref-5)
7. A. Bedi, [↑](#footnote-ref-6)
8. Forbes [↑](#footnote-ref-7)